ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)
On 21st & 22nd March Organized by

K.L.N. College of Engineering , Madurai, Tamil Nadu, India

Critical Analysis and Detection of Altered Fingerprints

Dr. K. Latha[#1], C. Manikandan[*2]

[#]Assistant professor, Department of CSE, Anna University (BIT Campus), Tiruchirappalli, India

[*]PG Scholar, Department of CSE, Anna University (BIT Campus), Tiruchirappalli., India

Abstract- The widespread operation of modified algorithm (National Institution of Standard Technology Fingerprint image Quality (NIFQ)) in government applications allow some persons with illegal environment by neglecting the detection of altered fingerprints. By using the fingerprint quality assessment software, it is difficult to find the altered fingerprints, since the quality of image does not degrade. This paper focuses on optimizing the modified NFIQ algorithm by implementing Neuro Fuzzy based on a large fingerprint image database. It can also be helpful in improving the performance by accuracy and robustness for detecting the fingerprint which is altered.

Keywords: Fingerprint, Neuro fuzzy, NFIQ, Altered Fingerprint, Optimize.

I. INTRODUCTION

Nowadays security is stepped to next extend, hence it is necessary to use fingerprint to protect the data. Many issues are identified such as altered fingerprints and fake fingerprints. To overcome the trouble, the NIST Fingerprint Image Quality (NFIQ) algorithm has become a standard method to access fingerprint image quality and to detect the altered fingerprint. Altered fingerprint is the fingerprint with some changes of the original fingerprint in small portion or otherwise large portion. It can be categorized into three types: 1) destruction 2) deformation 3) imitation. Fingerprint destruction is of friction ridge patterns on fingertips are obliterated by abrading, wounding, flaming, applying physically powerful chemicals, or transplanting soft skin. The scratched finger region needs to be sufficiently large to overcome fingerprint matchers. But, fingerprint quality control software can easily recognize such alterations at lowest quality level. The quality level five and one indicates poor, and excellent respectively.

The fingerprint deformation, friction ridge patterns on fingertips are twisted into abnormal edge patterns by a surgical method, in which portions of skin are removed from a finger and joined back in special positions. Distorted fingerprints may forward fingerprint quality control software as deformations do not essentially reduce the quality of the image. In fingerprint imitation, friction ridge skin from other parts of the body, such as fingers, palms, toes, and soles, is transplanted to the original finger in such a way that the altered fingerprint appears as a natural fingerprint pattern. These types of altered fingerprint patterns are obtained by the central region of the original fingerprint are replaced with the central region of a different portion. Imitated fingerprints can also be successfully restricted by fingerprint quality control software.

A. NFIQ Algorithm

In August 2004, NIST issued the NIST Fingerprint Image Quality (NFIQ) algorithm as part of the NIST Biometric Image Software (NBIS).NBIS software, categorizes into two types non export controlled and export controlled. The non-export controlled NBIS software includes five major packages: (PCASYS, MINDTCT, NFIQ, AN2K, and IMGTOOLS). The export controlled NBIS software includes two major packages: (NFSEG and BOZORTH3). The NFIQ algorithm is an open source tool for measuring the quality of fingerprint images independent of the fingerprint verification software used. The NFIQ measures quality by 5 classes, where class one refers to "excellent" and class five to "poor" refer to the class number of the input fingerprint. The NFIQ algorithm is based on an artificial neural network that tries to predict the quality class from 11 features of the image. These features include the numbers of minutiae and image blocks with quality index exceeding several thresholds. The neural network has been trained with a large number of fingerprint images and the corresponding comparison statistics obtained with different fingerprint verification software.

Notice that NFIQ has been designed to assign a level of quality to a grayscale fingerprint.

II. RELATED WORK

As per the concept of Anil K. Jain, Existing techniques was not able to identify the misused fingerprints. In this work, the system categorizes the alterations in an operational database into three types and also proposed automatic detection algorithm to identify altered fingerprints. This method was conducted on both real-world changed fingerprints and unnaturally generated changed fingerprints. It shows 7% of fake alarm rate and 92% of the changed fingerprints [1] [4].

According to the theory of J. Zhou, Fingerprint analysis is generally based on the location and outline of detected particular points in the images. These particular points (cores and deltas) not only explain the uniqueness of neighboring edge patterns but also conclude the fingerprint type and basically manage the orientation field. Novel technique was used. Disadvantages: This technique only support for singular point from the fingerprint image [3].

H. Cummins stated that fingerprint destruction, rubbing edge patterns on fingertips are destructed by abrading, wounding, flaming, applying physically powerful chemicals, or transplanting soft skin. The scratched finger region needs to be suitably large to defeat fingerprint matchers. But, fingerprint quality control software can easily identify such alterations at lowest quality level. Disadvantages: It only focus on destruction type, other types of altered fingerprint does not detect [2].

The theory of Jianjiang Feng, exclaims that recognition of alteration in basic fingerprints is additional popular than rolled fingerprints in non-forensic applications. After a misused fingerprint is detected, the process of effectively matching it next to the mated unaltered fingerprint, which is very feasible to be stored in the database, is very significant. In several types of altered fingerprints, such as destruction or small-area transplantation, edge patterns are scratched locally. It is feasible to restructure edge outline in the altered area using the unaltered edge sample in the locality. We have tried a stage model based approach to disrupt the misplaced or altered region [5].

III. PROPOSED WORK

It is proposed that detecting all types of altered fingerprints and fake fingerprints without leaving any other consideration. The modified NFIQ algorithm takes an input image that is in ANSI/NIST or NIST IHEAD format or compressed using WSQ, baseline JPEG, or lossless JPEG. The modified NFIQ produces the value of image quality for the image (where one is highest quality and five is lowest quality) and its output activation level from the neuro fuzzy.

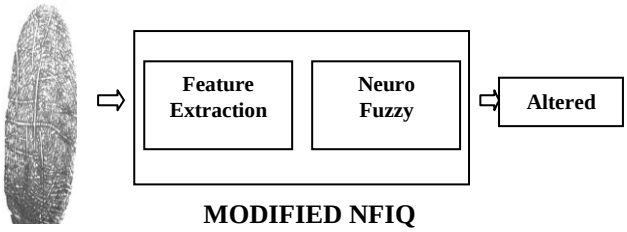

Fig 1 proposed block diagram

Feature extraction: This method computes the appropriate signal or image reliability characteristics and produces the results in a 11- dimensional feature vector. Minutiae detection system (MINDTCT) takes the finger print image as input and locates the feature in the ridges and furrows of the friction skin which is called as minutiae. The points are detected by the end of the ridges or splits. It stores the parameters such as location, type, orientation, and quality for searching. On a typical ten number of prints there are 100 minutiae are available. The matching process carries out on these points rather than the -50,000 pixels in the finger print image.

Extraction of Minutiae is for the determination of the location and for the of ridge bifurcations and terminations orientation. Minutiae Extraction is the next step of ridge extraction of the image. Then the minutiae points are to be extracted. If a ridge is only one pixel wide means, as a result, the fingerprint image is thinned. The points are minutiae which have value of a pixel is one as their neighbor ie; ridge ending or in their neighborhood, There is more than two ones ie (ridge bifurcations). This is the end process of minutiae points' extraction.

Neuro fuzzy This system uses a learning algorithm which is originally derived from neural network theory to establish its parameters (fuzzy sets and fuzzy rules) by processing data samples. The system focuses on 3-layer feed forward neural network which represents input variables, fuzzy rules output variables respectively. Fuzzy sets are commonly fixed as connection weights. It is not necessary for representing a fuzzy system to apply a learning algorithm to it. Moreover, it is fit, for the reason that it represents the data flow of input processing and learning within the model.

Algorithm

Step1: Input is feed into input layer, i.e., crisp input
Step2: Fuzzification of input crisp to membership fuzzy values
Step3: Rule evaluation (Fuzzy Rule Layer)
If (X1 is $A_{1)}$ AND (X_2 is B_1) THEN $f_1 = p_1x_1 + q_1x_2 + r_1$
If (X1 is A_2) AND (X2 is B_2) THEN $f_2 = p_2x_1 + q_2x_2 + r_2$
Step4: Output membership value (then part of rule)
Step5: Defuzzification layer (converting membership values to crisp value output)
Step6: Output is compared with target output (the process takes place until gets extract output)

Crisp Rules (input)

If x<a and y<b then $z=f_1$

FINGER PRINT

INPUT **OUTPUT**

If x<a and y<b then $z=f_2$
If x<a and y<b then $z=f_3$
If x<a and y<b then $z=f_4$

Weight is adjusted till there is equal to target output. Reduction of rules takes place, NN is used to select the higher rule and fuzzy is used for prove that the rule is high in strength.

Characteristics

There are two main characteristics of fuzzy systems that give better performance for specific applications.

- Fuzzy systems are suitable for uncertain or fairly accurate analysis, mostly for the system with a mathematical model that is complicated to receive.
- Fuzzy logic allows decision making with expected values under unfinished or uncertain information.

IV. EXPERIMENTAL RESULTS

Four fingerprint images such as original fingerprint and three types of altered fingerprints (obliterated, distorted, imitated) of the first 1,000 fingerprints in SD4 are used to train neuro fuzzy. The residual 976 fingerprints and its altered versions are used to test the modified NFIQ algorithm. The normalized score is termed as fingerprint-ness. When the fingerprint-ness of an input image is smaller than a predetermined threshold, system raises an alarm for altered fingerprints. If this image is indeed an altered fingerprint, it is a true detection; otherwise it is a false alarm.

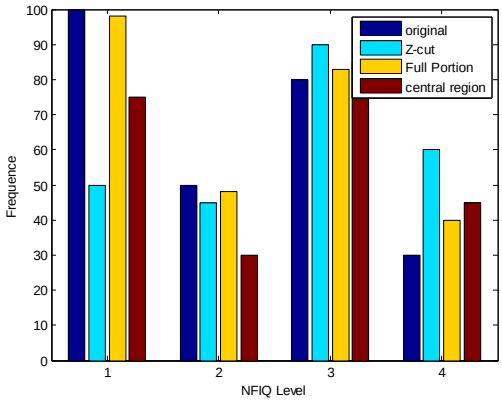

Fig. 2 distribution of NFIQ

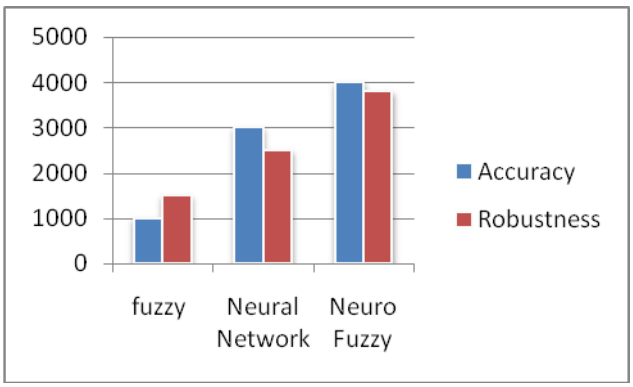

Fig. 3 Performance metrics

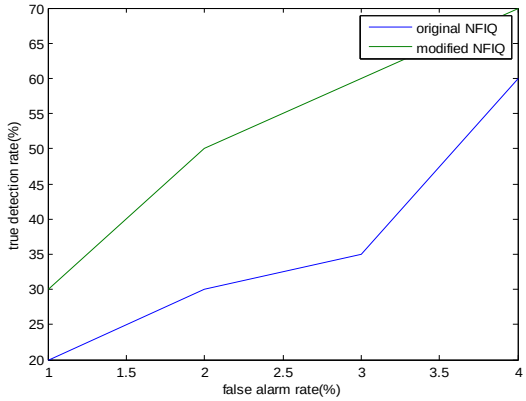

Fig. 4 ROC Curve of NFIQ and modified NFIQ

V. CONCLUSION

In this work it is concluded that analyzing and detecting the altered fingerprints identification. Some of the types of altered fingerprints cannot be identified by the NFIQ. To overcome the problem, the algorithm optimizes with neuro fuzzy technique. For the future work it is expected to generalize the NFIQ algorithm in order to use within governmental fingerprint enrolment and authentication scenarios.

REFERENCES

[1] J. Feng, A.K. Jain, and A. Ross, "Detecting Altered Fingerprints," Proc. 20th Int'l Conf. Pattern Recognition, pp. 1622-1625, Aug. 2010.

[2] H. Cummins, "Attempts to Alter and Obliterate Finger-prints," J. Am. Inst. Criminal Law and Criminology, vol. 25, pp. 982-991.

[3] J. Zhou and J. Gu, "A Model Based Method for the computation of Fingerprints' Orientation Field," IEEE Trans. Image Processing, vol. 13, no. 6, pp. 821-835, 2004.

[4] E. Tabassi, C. Wilson, and C. Watson, "Fingerprint Image Quality," NISTIR 7151, http://fingerprint.nist.gov/NFIS/ir_7151.pdf, Aug. 2004.

[5] Jianjiang Feng, A. K. Jain, A. Ross, "Fingerprint Alteration", MSU Technical Report, MSU-CSE-09-30, Dec. 2009

[6] Abraham A & Nath B, Designing Optimal Neuro- Fuzzy Systems for Intelligent Control, In proceedings of the Sixth International Conference on Control Automation Robotics Computer Vision, (ICARCV 2000), Singapore, December 2000.

[7] J. Zhou, F. Chen, and J. Gu, "A Novel Algorithm for Detecting Singular Points from Fingerprint Images," IEEE PAMI, vol. 31,no. 7, pp. 1239–1250, 2009.

[8] S. Wood, C. Wilson, “Studies of Plain-to-Rolled Fingerprint Matching Using the NIST Algorithmic Test Bed (ATB),” Technical Report NISTIR 7112, April 2004. http://www.itl.nist.gov/iad/894.03/pact/pact.html.

[9] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition (Second Edition). Springer-Verlag, 2009.

[10] J. C. Wu, C. Wilson, "Nonparametric Analysis of Fingerprint Data", 7226, National Institute for Standard and Technology, 2005.

[11] International Organization for Standardization, "ISO/IEC 19795-1 – Information technology - Biometric performance testing and reporting - Part 1: Principles and framework", 2006.